IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants(s)	: WANKMUELLER, John	Examiner	: KESACK, Daniel
Serial No.	: 09/783,775	Confirmation No.	: 2264
Filed	: February 15, 2001	Group Art Unit	: 3691
For	: SYSTEM AND METHOD FOR CONDUCTING ELECTRONIC COMMERCE WITH A REMOTE WALLET SERVER		

APPEAL BRIEF

TABLE OF CONTENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants(s)	: WANKMUELLER, John	Examiner	: KESACK, Daniel
Serial No.	: 09/783,775	Confirmation No.	: 2264
Filed	: February 15, 2001	Group Art Unit	: 3691
For	: SYSTEM AND METHOD FOR CONDUCTING ELECTRONIC COMMERCE WITH A REMOTE WALLET SERVER		

APPEAL BRIEF

Commissioner for Patents
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal brief is being filed further to the notice of appeal dated April 30, 2010. The claims have been six times rejected, in a non-final office action dated September 30, 2005, a final office action dated February 27, 2006, a non-final office action dated November 17, 2006, a final office action dated May 4, 2007, a non-final office action dated March 5, 2009, and a final office action dated November 30, 2009.

Applicant authorizes the Director to charge the appropriate fee, and credit any overpayment, to Deposit Account No. 02-4377.

I. REAL PARTY IN INTEREST

The real party in interest is Mastercard International Incorporated, the assignee of the entire right, title, and interest in the present application by way of Assignment recorded June 19, 2000 at reel/frame 010931/0323.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF CLAIMS

Claims 2-6, 8, and 10 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Gray et al., U.S. Patent No. 7,366,703 ("Gray"), further in view of the EMV '96 Chip Electronic Commerce Specification, version 1.0 ("EMV96") and Chen, U.S. Patent No. 5,590,197 ("Chen"). Claims 1, 7, and 9 have been previously canceled without prejudice.

IV. STATUS OF AMENDMENTS

Specification

None.

Claims

None.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present application relates generally to a system and method for conducting online commerce with a remote wallet server. (*See, e.g.*, Specification, page 1 lines 1-2[1]).

Independent claim 2 is directed to a method for conducting a payment transaction over a computer network between a consumer and a merchant involving a payment card issued by an issuer institution to the consumer, wherein the computer network includes at least three computers connected thereto, a consumer computer operated by or on behalf of the consumer, a merchant computer operated by or on behalf of the merchant, and a wallet server at a location remote from said consumer that provides functionality for the consumer computer to conduct transactions over the computer network, and wherein the payment card is in a form of either a chip card or a non-chip card, the method comprising:

receiving a request at a remote wallet server from the consumer computer for conducting a payment function with the merchant computer; [exemplary support for these limitations may be found at, *e.g.*, specification, page 10 line 7- page 11 line 2]

in response to the request, conducting the payment transaction by the remote wallet server with the merchant computer in a format compliant with a chip card electronic commerce protocol or specification, wherein the remote wallet server and the issuer institution have a shared secret data object; [exemplary support for these limitations may be found at, *e.g.*, specification, page 11 lines 3-20]

---

1 Page and line numbers refer to the application as filed.

generating a cryptogram by the remote wallet server based on the shared secret data object between the remote wallet server and the issuer institution; and [exemplary support for these limitations may be found at, *e.g.*, specification, page 11 lines 3-12]

sending payment-related information and the cryptogram by the remote wallet server to the merchant computer in response to the request by the consumer computer. [exemplary support for these limitations may be found at, *e.g.*, specification, page 11 line 13 - page 12 line 3]

Independent claim 3 and its corresponding dependent claims 4 and 5 are directed to a remote wallet server for facilitating a payment transaction over a computer network between a consumer and a merchant, wherein the transaction involves a payment card issued by an issuer institution to the consumer, wherein the payment card is in a form of either a chip card or a non-chip card, and wherein the computer network includes at least three computers connected thereto, a consumer computer operated by or on behalf of the consumer, a merchant computer operated by or on behalf of the merchant, and the wallet server at a location remote from said consumer, the remote wallet server comprising:

a microprocessor unit; [exemplary support for these limitations may be found at, *e.g.*, specification, claim 3]

a memory unit coupled to the microprocessor unit; [exemplary support for these limitations may be found at, *e.g.*, specification, claim 3]

means for conducting a payment function between the remote wallet server and the merchant computer in response to a request for such a function by the consumer computer wherein the payment transaction is conducted in a format compliant with a chip card electronic commerce protocol or specification. [Appellant hereby identifies this limitation as a means plus

function limitation as permitted under 35 U.S.C. § 112, sixth paragraph. Exemplary support for these limitations may be found at, *e.g.*, specification, page 7 lines 6-14; page 9 lines 1-6; page 10 line 7 - page 12 line 3; Fig. 2]

Independent claim 6 is directed to a method for conducting a payment transaction over a computer network between a consumer and a merchant involving a payment card issued by an issuer institution to the consumer, wherein the payment card is in a form of either a chip card or a non-chip card, wherein the computer network includes at least three computers connected thereto, a consumer computer operated by or on behalf of the consumer, a merchant computer operated by or on behalf of the merchant, and a wallet server at a location remote from said consumer that provides functionality for the consumer computer to conduct transactions over the computer network, wherein the remote wallet server and the issuer institution have a shared secret data object, the method comprising:

receiving a request at a remote wallet server from the consumer computer for conducting a payment function with the merchant computer; [exemplary support for these limitations may be found at, *e.g.*, specification, page 10 line 7- page 11 line 2]

generating a cryptogram by the remote wallet server based on the shared secret data object between the remote wallet server and the issuer institution, regardless of whether or not the payment card of the consumer involved in the payment transaction is a chip card or a non-chip card; and [exemplary support for these limitations may be found at, *e.g.*, specification, page 11 lines 3-12; page 12 lines 4-12]

sending payment-related information and the cryptogram by the remote wallet server to the merchant computer in response to the request by the consumer computer, wherein the

payment-related data and the cryptogram are transmitted in a format compliant with a chip card electronic protocol or specification. [exemplary support for these limitations may be found at, *e.g.*, specification, page 11 line 13 - page 12 line 3]

Independent claim 8 and its corresponding dependent claim 10 are directed to a remote wallet server for facilitating a payment transaction over a computer network between a consumer and a merchant involving a payment card issued by an issuer institution to the consumer, wherein the payment card is in a form of either a chip card or a non-chip card, wherein the computer network includes at least three computers connected thereto, a consumer computer operated by or on behalf of the consumer, a merchant computer operated by or on behalf of the merchant, and the wallet server at a location remote from said consumer, comprising:

a microprocessor unit; [exemplary support for these limitations may be found at, *e.g.*, specification, claim 8]

a memory unit coupled to the microprocessor unit; [exemplary support for these limitations may be found at, *e.g.*, specification, claim 8]

a storage unit having stored therein a secret data object that is shared with the issuer institution; [exemplary support for these limitations may be found at, *e.g.*, specification, page 9 lines 1-6]

means for generating a cryptogram by the remote wallet server based on the secret data that is shared between the remote wallet server and the issuer institution, regardless of whether or not the payment card of the consumer involved in the payment transaction is a chip card or a non-chip card; and [Appellant hereby identifies this limitation as a means plus function limitation as permitted under 35 U.S.C. § 112, paragraph 6. Exemplary support for these

limitations may be found at, *e.g.*, specification, page 7 lines 7-14; page 9 lines 1-6; page 11 lines 3-12; step 1050 of Figure 2]

application code stored in the memory unit for sending payment-related information and the cryptogram to the merchant computer in response to a request by the consumer computer to conduct a payment function with the merchant computer wherein the application code includes means for transmitting the payment-related information and the cryptogram in a format compliant with a chip card electronic commerce protocol or specification. [Appellant hereby identifies the "means for transmitting..." limitation as a means plus function limitation as permitted under 35 U.S.C. § 112, sixth paragraph. Exemplary support for these limitations may be found at, *e.g.*, specification, page 7 lines 12-14; page 11 line 13 - page 12 line 2; step 1060 of Figure 2]

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The rejection of claims 2-6, 8, and 10 under 35 U.S.C. § 103(a) as recited in the final office action dated November 30, 2009.

VII. ARGUMENT

In this appeal brief, Appellant presents arguments concerning the patentability of claims 2-6, 8, and 10 to address the Examiner's rejections. Appellant's silence with regard to any aspect of the Examiner's rejections of the dependent claims constitutes recognition by the Appellant that the rejections are moot based on Appellant's remarks relative to the independent claim from which the dependent claims depend.

Rejection Of Claim 2 Under 35 U.S.C. § 103

"Where the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it." MPEP § 707.07(f). Where an applicant's arguments are not addressed by the examiner, the arguments are deemed to be persuasive. "The court noted that since applicant's statement of advantages was not questioned by the examiner or the Board of Appeals, it was constrained to accept the statement at face value and therefore found certain claims to be allowable. See also *In re Soni*, 54 F.3d 746, 751, 34 USPQ2d 1684, 1688 (Fed. Cir. 1995) (Office failed to rebut applicant's argument)." MPEP § 707.07(f) (citing *In re Herrmann*, 261 F.2d 598 (C.C.P.A. 1958)). At the outset, Appellant respectfully submits that the final office action dated November 30, 2009 ("Final Office Action") does not fully address the arguments set forth in Appellant's response dated July 29, 2009 ("Response"). Accordingly, the arguments should be deemed persuasive.

Appellant argued, in the Response:

> Applicant respectfully traverses the Office Action's conclusion that one of ordinary skill in the art would understand it to be obvious to apply card-present payment techniques from consumer to merchant using a chip-card reader found in the EMV96 specification to the mediated e-commerce transaction techniques of wallet servers. The Office Action fails to appreciate the additional,

> non-trivial problems that occur when conducting chip card transactions with a merchant on behalf of a consumer or other entity over the internet, for example, authenticating the intermediary in view of large numbers of consumers served by the intermediary (specification Paras. [0009]-[0010]) and management and security of potentially large numbers of keys and/or certificates (specification Para. [0011]). Nowhere does Gray or EMV96 include teachings that would lead one of ordinary skill in the art to solve these non-trivial problems which are using the claimed techniques.

Response, p. 10.

Even assuming that the Final Office Action properly addresses Appellant's arguments, Appellant respectfully submits that neither *Gray*, *EMV96*, nor *Chen*, taken alone or in combination, discloses or suggests the subject matter of claim 2. Appellant respectfully traverses the Office Action's conclusion that one of ordinary skill in the art would understand it to be obvious to apply card-present payment techniques from consumer to merchant using a chip-card reader found in the EMV96 specification to the mediated e-commerce transaction techniques of wallet servers.

One of ordinary skill would not understand EMV96 to teach or suggest mediating transactions (e.g., a function of a wallet server). Even assuming that EMV96 teaches a Chip Card Protocol, the EMV96 protocol allows for transactions directly between a chip card and a merchant, not between an intermediary wallet server and the merchant on behalf of a customer. The Examiner states that EMV96 concerns transactions between a payment source and a payment receiving system. Office Action, p. 6 ("The specification defines a protocol for conducting a transaction between a payment source and a payment receiving system." (emphasis added)). The claimed invention, however, involves a wallet server at a location remote from the

consumer, which is a payment intermediary, not a payment source. It facilitates payment transactions on behalf of a consumer rather than initiating payment transactions.

As EMV96 makes clear, the transactions contemplated by the specification occur between a payment source and the merchant, not via an intermediary acting on behalf of the consumer and the merchant. The Cardholder System in EMV96 is the entity which directly interfaces with the integrated chip card. EMV96, Table 3, p.10. The "Cardholder System [s]erves as the interface between the EMV IC Card and the SET merchant server. It is responsible for authenticating the merchant to the cardholder." Id. p.2. The Cardholder System is at the location of the Cardholder (i.e., the consumer). Nothing in EMV96 suggests that the Cardholder System interfaces with an intermediary wallet server or that the Cardholder System itself is an intermediary wallet server. Therefore, according to the Office Action and the EMV96 specification, EMV96 describes only direct communications between a consumer and a merchant. Nothing in EMV96, therefore, discloses or suggests a wallet server at a location remote from the consumer.

Appellant respectfully submits that the Office Action does not appreciate the additional, non-trivial problems that occur when conducting chip card transactions with a merchant on behalf of a consumer or other entity over the internet, for example, authenticating the intermediary in view of large numbers of consumers served by the intermediary (specification Paras. [0009]-[0010]) and management and security of potentially large numbers of keys and/or certificates (specification Para. [0011]). Nowhere does Gray or EMV96 include teachings that would lead one of ordinary skill in the art to solve these non-trivial problems which are resolved

by using the claimed techniques. Accordingly, Appellant requests reversal of the rejections of claim 2.

Rejection Of Claims 3-5 Under 35 U.S.C. § 103

Claim 3 include similar features as claim 2. Accordingly, Appellant requests reversal of the rejection of claims 3 for at least the same reasons as claim 2. Claims 4 and 5 depend from claim 3. Appellants request reversal of the rejections of claims 4 and 5 for at least the same reasons as claims 3.

Rejection of Claim 6 Under 35 U.S.C. § 103

Claim 6 is directed to a method for conducting a payment transaction over a computer network. Claim 6 includes similar features as claim 2 and the rejection of claim 6 should be reversed for at least the same reasons as discussed above in relation to claim 2. In addition, the cited references fail to disclose or suggest, among other things, "generating a cryptogram by the remote wallet server based on the shared secret data object between the remote wallet server and the issuer institution, regardless of whether or not the payment card of the consumer involved in the payment transaction is a chip or a non-chip card," as recited in claim 6.

Gray is directed to a system and method for conducting electronic commerce. *See* Gray, Abstract. "When a purchase is to be consummated, user 110 accesses wallet server 140 [and] is then directed...to insert a Smart Card into, for example, a card reader system to verify that a Smart Card is in the user's possession." Gray, Col. 7 lines 8-11. Therefore, even assuming that the combination of Gray and Chen would disclose or suggest the generation of a cryptogram, such cryptogram would not be generated when the card is a non-chip card because Gray requires a smart card (i.e., a chip card) for authentication.

As such, and in addition to the reasons set forth above in relation to claim 2, the cited references fail to disclose or suggest, among other things, "generating a cryptogram by the remote wallet server based on the shared secret data object between the remote wallet server and the issuer institution, regardless of whether or not the payment card of the consumer involved in the payment transaction is a chip or a non-chip card," as recited in claim 6. Appellant therefore respectfully requests that the rejection be reversed and claim 6 be allowed.

Rejection Of Claims 8 and 10 Under 35 U.S.C. § 103

Claim 8 include similar features as claim 6. Accordingly, Appellant requests reversal of the rejection of claims 8 for at least the same reasons as set forth above in relation to claim 6. Claim 10 depends from claim 8. Appellants request reversal of the rejections of claim 10 for at least the same reasons as claims 8.

VIII. CLAIMS APPENDIX

The rejection of the following claims 2-6, 8, and 10 is appealed.

1. Canceled.

2. A method for conducting a payment transaction over a computer network between a consumer and a merchant involving a payment card issued by an issuer institution to the consumer, wherein the computer network includes at least three computers connected thereto, a consumer computer operated by or on behalf of the consumer, a merchant computer operated by or on behalf of the merchant, and a wallet server at a location remote from said consumer that provides functionality for the consumer computer to conduct transactions over the computer network, and wherein the payment card is in a form of either a chip card or a non-chip card, the method comprising:

receiving a request at the remote wallet server from the consumer computer for conducting a payment function with the merchant computer;

in response to the request, conducting the payment transaction by the remote wallet server with the merchant computer in a format compliant with a chip card electronic commerce protocol or specification, wherein the remote wallet server and the issuer institution have a shared secret data object;

generating a cryptogram by the remote wallet server based on the shared secret data object between the remote wallet server and the issuer institution; and

sending payment-related information and the cryptogram by the remote wallet server to the merchant computer in response to the request by the consumer computer.

3. A remote wallet server for facilitating a payment transaction over a computer network between a consumer and a merchant, wherein the transaction involves a payment card issued by an issuer institution to the consumer, wherein the payment card is in a form of either a chip card or a non-chip card, and wherein the computer network includes at least three computers connected thereto, a consumer computer operated by or on behalf of the consumer, a merchant computer operated by or on behalf of the merchant, and the wallet server at a location remote from said consumer; the remote wallet server comprising:

a microprocessor unit;

a memory unit coupled to the microprocessor unit;

means for conducting a payment function between the remote wallet server and the merchant computer in response to a request for such a function by the consumer computer wherein the payment transaction is conducted in a format compliant with a chip card electronic commerce protocol or specification.

4. The remote wallet server of claim 3, further comprising:

a storage unit having stored therein a secret data object that is shared with the issuer institution;

means for generating a cryptogram by the remote wallet server based on the secret data that is shared between the remote wallet server and the issuer institution; and

application code stored in the memory unit for sending payment-related information and the cryptogram to the merchant computer in response to the request by the consumer computer to conduct the payment transaction with the merchant computer.

5. The remote wallet server of claim 4, wherein the storage unit and the means for generating a cryptogram are contained in a tamper-resistant security module.

6. A method for conducting a payment transaction over a computer network between a consumer and a merchant involving a payment card issued by an issuer institution to the consumer, wherein the payment card is in a form of either a chip card or a non-chip card, wherein the computer network includes at least three computers connected thereto, a consumer computer operated by or on behalf of the consumer, a merchant computer operated by or on behalf of the merchant, and a wallet server at a location remote from said consumer that provides functionality for the consumer computer to conduct transactions over the computer network, wherein the remote wallet server and the issuer institution have a shared secret data object, the method comprising:

receiving a request by the remote wallet server from the consumer computer for conducting a payment function with the merchant computer;

generating a cryptogram by the remote wallet server based on the shared secret data object between the remote wallet server and the issuer institution, regardless of whether or not the payment card of the consumer involved in the payment transaction is a chip card or a non-chip card; and

sending payment-related information and the cryptogram by the remote wallet server to the merchant computer in response to the request by the consumer computer, wherein the payment-related information and the cryptogram are transmitted in a format compliant with a chip card electronic commerce protocol or specification.

7. Canceled.

8. A remote wallet server for facilitating a payment transaction over a computer network between a consumer and a merchant involving a payment card issued by an issuer institution to the consumer, wherein the payment card is in a form of either a chip card or a non-chip card, wherein the computer network includes at least three computers connected thereto, a consumer computer operated by or on behalf of the consumer, a merchant computer operated by or on behalf of the merchant, and the wallet server at a location remote from said consumer, comprising:

a microprocessor unit;

a memory unit coupled to the microprocessor unit;

a storage unit having stored therein a secret data object that is shared with the issuer institution;

means for generating a cryptogram by the remote wallet server based on the secret data that is shared between the remote wallet server and the issuer institution, regardless of whether or not the payment card of the consumer involved in the payment transaction is a chip card or a non-chip card; and

application code stored in the memory unit for sending payment-related information and the cryptogram to the merchant computer in response to a request by the consumer computer to conduct a payment function with the merchant computer wherein the application code includes means for transmitting the payment-related information and the cryptogram in a format compliant with a chip card electronic commerce protocol or specification.

9. Canceled.

10. The remote wallet server of claim 8, wherein the storage unit and the means for generating a cryptogram are contained in a tamper-resistant security module.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.

For at least the foregoing reasons, the rejections of claims 2-6, 8, and 10 should be reversed.

Respectfully submitted,

Dated: November 30, 2010

By: _____

Eliot D. Williams
Patent Office Reg. No. 50,822

Brian Boerman
Patent Office Reg. No. 66,678

Attorneys for Appellant
Telephone: (212) 408-2517

Baker Botts L.L.P.
30 ROCKEFELLER Plaza
New York, NY 10112-4498